**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

* Data integrity is the assurance that data is accurate and reliable and Is available in a timely manner.

1. Biometrics
   1. Describe biometric security.

* Biometric security is the use of physical or behavioural human characteristics to authenticate a user before granting them access to data.
  1. Why does it appeal to security managers?
* It appeals to security managers because it is nearly impossible to copy or steal a person’s biometric characteristics.
  1. List the common biometric devices.
* Voice recognition
* Fingerprint recognition
* Hand geometry
* Signature verification
* Iris recognition
  1. What are the concerns of biometric technology?
* Biometric technology is very expensive so organisations will have to weight up the threats against the cost of installing these security devices.

1. Swipe cards
   1. Describe the nature of a swipe card.

* A swipe card is a business card sized plastic card with a magnetic strip on one side and on the other contains the user’s details. The magnetic strip contains information about the owner of the card including a personal identification number or pin. Swipe cards can be used for electronic transactions such as paying for the groceries.
  1. What is a limitation of the swipe card?
* A swipe card can be easily damaged by magnetic fields. If stolen they offer little protection from a thief with a swipe-card reader that can capture the data in it.

1. Smart cards

* Smart cards look like swipe cards except that it has a microchip embedded in it to store and manipulate data. Common smart cards include prepaid telephone cards, photocopy cards and the new Myki public transport ticketing.

1. Security tokens

* Security tokens are a small device about the size of a key ring may be used to display a constantly changing authentication code. When users wish to access information they need to enter their account name, their password and then the authentication code is displayed on the security token.

1. Mobile phone secure code
   1. How does this level of authentication work?

* Authentication occurs when a security code is sent to the account holder’s mobile phone to authenticate a transaction before it actually occurs. The account holder then needs to log in and enter the code before the transaction is processed.

**Power protection**

Outline the characteristics of the following:

1. Surge protector

* A surge protector protects electrical equipment against overvoltage caused by a power surge. It smooths the current coming from the mains supply and will block sudden surges known as spikes.

1. Uninterruptible power supply, (UPS)

* A UPS is a high quality surge protector and battery built into the one device. Not only does it guard against spikes but it will also help to protect data if there is an undercurrent or complete power failure.

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?

* Redundancy means building in extra items that are not strictly necessary for something to function as a backup.

1. What is meant be a fault-tolerant server?

* A fault-torrent server will continue to work even when a piece of hardware has failed. This tolerance is achieved by having multiple components such as dual hard drives, motherboards or power transformers running in parallel. Technicians can repair the system without interrupting its basic operation.

1. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.

* No single part of the system is critical to its overall operation. If one part fails the others can just take over its job and keep the system running until the part is replaced.
  1. What is meant by RAID technology
* Redundant array of inexpensive disks (RAID) is normally used on a computer network. In a RAID protected system fragments of data are spread over several hard drives so that if one hard drive fails the others can piece together the missing data and rebuild the file using error checking codes.

1. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

* RAID is used because if the main computer fails RAID will instantly take over and attempt to restart it and put the failed machine back online within thirty seconds.

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

* Cost of the drive or writer
* Cost of the media per GB
* Speed and compatibility

Three categories of backup media:

* Magnetic media
* Optical drives
* Solid-state drives

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive

* Affordable
* Useful if you have many files
* Best to have a removable or external hard disk

1. Magnetic tapes

* Cheap
* Very slow to save and restore files

**Optical media**

1. Compact disc

* Removable storage can hold up to 700MB
* Come as CDs
* Allows you to write data to the disc a number of times

1. DVD

* Can store up to 17GB
* Can either be used once or used many times

1. Blu-ray

* Capacity of 50GB
* Designed to replace DVDs
* Blu-ray refers to the blue laser used to read the disc

**Solid-state drives**

1. USB storage devices

* Popular way of backing up files
* Can take anywhere
* Can hold up to 256GB
* Ranging from single purpose to multi-purpose devices

**Online backups**

1. Why do organisations use this form of backup?

* Organisations use this form to ensure that they work as effectively and efficiently as possible.

1. Describe an enterprise storage system.

* An enterprise storage system typically involves the interconnection via a storage area network (SAN) of RAID disks, tapes, CD/DVD-ROM servers, internet backup and other networked storage devices.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers

* Packet sniffers are diagnosed tools that monitor the contents of packets of data being sent across networks.

1. Desktop monitoring programs

* See what is on the desktop
* All tasks are logged
* Hackers use these

1. Log files

* Websites record every URL accessed, web browsers store webpages, network, etc.

1. Closed-circuit television, (CCTV)

* CCTV consists of a series of video cameras linked to an internal TV system.

1. Telephones

* Supervisors may want to ensure that phone calls are restricted to company business
* Call centres designed for customer service might also monitor calls to ensure that a high standard of service is actually being provided

1. Audit trails

* Enables managers to trace transactions or any other form of activity in its system